NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Authorities investigate Tuesday oil rig explosion. One man was sent to the hospital in critical condition after an oil rig explosion September 4 in Mountrail County, North Dakota. The Mountrail County Sheriff's Department reported that a 9-1-1 call was received from a Hess Oil Rig, 12 miles southwest of Stanley. The oil worker fell from the top of a tank after the explosion. Ninety percent of his body sustained burns. The man was flown to a local hospital and then transferred to a burn unit at a hospital in Minnesota. The cause of the fire is unknown at this time. The Mountrail County Sheriff's Department along with the oil field company that the victim is employed by, are continuing their investigations into the accident. Source: http://www.kfyrtv.com/News_Stories.asp?news=59131

Hot, dry conditions continue to speed up row crops. Hot, dry conditions across North Dakota have spurred crop development in the State, but fall tillage may be put on hold due to a lack of moisture, the Associated Press reported September 4. The U.S. Department of Agriculture said in its weekly crop report that Durum wheat was 92 percent harvested while Canola was at 91 percent. Eighty percent of corn was dented, which is well ahead of the average of 37 percent. Topsoil moisture was rated 19 percent very short, 53 percent short, and 28 percent adequate. Pasture and range conditions were rated 16 percent very poor, 31 percent poor, 36 percent fair, and 17 percent good. Source: http://bismarcktribune.com/news/state-and-regional/hot-dry-conditions-continue-to-speed-up-row-crops/article_ef8fa6aa-f709-11e1-9cbe-001a4bcf887a.html?comment_form=true

2 more dams on the Red River in eastern North Dakota modernized in $1.7 million project. Officials completed a $1.7 million project to modify two dams on the Red River near Oxbow, North Dakota. The Forum of Fargo-Moorhead newspaper reported the dams at Hickson and Christine were renovated to enhance fish passage and improve safety. Fargo owns the two dams, as well as three others on the river. All five have now been modified to reduce the risk of drowning deaths. Only one of the eight dams on the Red south of the Canadian border still must be modernized. An upgrade to the dam at Drayton is planned as part of the Red River diversion project in the Fargo area and once completed, fish will have 600 miles of free-flowing river to navigate. Source: http://www.therepublic.com/view/story/591e6f8b494c4c2f9451d36f0a025475/ND--Dams-Modernized

Regional

(Minnesota) **New basil fungal disease found in Minnesota.** Minnesota gardeners who grow basil for cooking should be aware of a new fungal disease that attacks the herb, the Associated Press reported September 5. The Minnesota Department of Agriculture confirmed the State's first case of basil downy mildew. The disease damages leaves, resulting in unmarketable plants. The fungus can affect basil grown in gardens as well as in commercial greenhouses. The disease is spread by infected seed in transplants as well as by windblown spores. Source: http://www.sacbee.com/2012/09/05/4787943/new-basil-fungal-disease-found.html

National

Nothing Significant to Report

International

US embassy evacuated after Brussels bomb scare. The U.S. embassy and several Belgian government offices were evacuated September 5 after police found a suspect vehicle nearby but they later lifted the alert after a search. Police said a patrol noticed a suspicious vehicle around midday and called in the bomb squad, informing the U.S. embassy, which decided to evacuate staff as a precaution, including from the U.S. mission to the European Union, according to a mission spokesman. Police said the U.S. action was taken independently as a precaution while authorities ordered the evacuation of Belgian government offices. —There was nothing in the car, nothing suspect, a police spokeswoman said. —Given the area, however, we did not want to take any risk and so the army bomb squad was called in, she added. The alert disrupted traffic in central Brussels near the royal palace, an area that is home to many of the larger embassies. Source: http://www.google.com/hostednews/afp/article/ALeqM5jbt6cckP2YY0Rqe1z1lUSLlnSxIw?docId=CNG.229e1ed397ce2fca388f424f0c2cc3ea.181

Chemical reaction sparks alert at French nuclear plant. A chemical reaction at the Fessenheim nuclear power plant in Strasbourg, France injured two staff and triggered a brief fire alert September 5, local government and fire service officials said. The incident, sparked by a chemical reaction, was quickly brought under control, the officials at the local government prefect's office and the fire services said. French power utility EDF, which operates the plant, said there had been a steam leak there but denied initial reports from the local fire brigade that a fire had broken out. —Steam escaped during a maintenance operation which set off the fire alarm, a spokeswoman said. Source: http://www.chicagotribune.com/news/sns-rt-us-france-nuclear-accidentbre88410b-20120905,0,4295327.story

Coast Guard requires heightened security for ships that call on Yemeni ports. Starting September 18, ships that visit all but a handful of Yemeni seaports within five port calls of entering the United States must carry out heightened security measures under new Coast Guard regulations printed September 4 in the Federal Register, Fierce Homeland Security reported September 2. The rules came about following a Coast Guard finding that Yemeni ports do not maintain effective anti-terrorist measures along with an assessment that Yemen presents a significant risk of introducing instruments of terror into maritime commerce. As a result, ships having docked in any Yemeni port excepting the Ash Shihr oil terminal, the Balhalf liquid natural gas terminal, and the port of Hodeidah, also known as al Hudaydah, during their past five ports of call must notify the Coast Guard prior to arrival into U.S. waters and report on heightened security measures undertaken while docked in Yemen. Source: http://www.fiercehomelandsecurity.com/story/coast-guard-requires-heightened-security-ships-call-yemeni-ports/2012-09-02

Banking and Finance Industry

Insider security threat gets a serious look by US security agencies. A study, —Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector funded by the DHS in collaboration with the U.S. Secret Service and the U.S. Computer Emergency Readiness Team Insider Threat Center, part of Carnegie Mellon University's Software Engineering Institute looked at what they called technical and behavioral patterns from 67 insider and 13 external fraud cases that occurred between 2005 and 2012 to develop —insights and risk indicators of malicious insider activity, NetworkWorld reported September 6. The study developed findings on insider threats to financial institutions including methods of insider fraud and theft. These included that most insiders did not use very technically sophisticated methods, that more than half of the cases used some form of authorized access, and that most incidents were detected through an audit, customer complaint, or coworker suspicion, among other findings. Source: http://www.networkworld.com/community/node/81342

Online banking trojan has designs on chipTAN users. The Tatanga trojan has come up with a new way of ripping off online banking users in Germany by deceiving users of the chipTAN system, The H reported September 6. Transaction authentication numbers (TAN), are one-time authentication numbers generated and used to validate banking transactions. Tatanga already had a reputation for attacking mobile TAN systems (mTAN) that use SMS to send through a TAN number. ChipTAN is a different system that requires a bank card to be inserted into a device and then held against the screen. The bank then flashes the display to transfer data about the current transaction to the device, which generates a TAN for the current transaction. According to Trusteer, Tatanga can get the TAN number from a chipTAN user by tricking them into thinking the bank is testing the chipTAN system. When a user logs into their bank account, the trojan checks the user's account details and selects an account from which it can take the most money. It then begins a transfer, but to complete that transfer it needs a TAN. Tatanga injects code into the user's bank Web browsing explaining the bank is performing a chipTAN test. If the user follows the instructions, they enter a TAN number into the system that Tatanga uses to complete its transaction. When the transaction is complete, Tatanga takes steps to obscure the transaction in the victim's transaction history. Source: http://www.h-online.com/security/news/item/Online-banking-trojan-has-designs-on-chipTAN-users-1701688.html

U.S. SEC charges China Sky One with securities fraud. The U.S. Securities and Exchange Commission (SEC) charged China Sky One Medical Inc and its chief executive with securities fraud and said the company recorded fake sales of a weight loss product, Reuters reported September 4. China Sky One inflated revenues in its financial statements by booking $19.8 million in phony export sales, the SEC said. The company, based in China, said in 2007 securities filings it had entered into a distribution agreement with a Malaysian company that would generate the sales, but never entered into such an agreement. The company's chief executive certified the overstated financial results, which appeared in financial statements through 2010. The case is the latest in a series of actions the SEC has taken against Chinese companies listed in the U.S. Dozens of such companies, which often go public by merging with shell companies,

have disclosed auditor resignations or bookkeeping irregularities. The company's auditor, MSPC, resigned in March after one of the company's directors resigned and said he was having trouble getting in touch with the company's finance executives. Source: http://reuters.com/article/2012/09/04/skyone-sec-fraud-idINL2E8K4BAR20120904

(California) **Kidnappers strapped device to bank employee for East LA robbery: LASD.** Two men wearing ski masks kidnapped a bank employee held her overnight, attached a supposed bomb to her and then had her rob an East Los Angeles bank, according to the Los Angeles County Sheriff's Department (LASD). She was abducted from her home in Huntington Park, California, September 4, an LASD captain said. The morning of September 5, the woman was at a Bank of America branch in Los Angeles, he said. —She went into the bank, and she told another employee or employees that she had this device attached to her, and that she was demanded by the robbers to (get) the money from the bank and throw it outside. A SWAT team, bomb squad, sheriff's deputies, and the fire department responded to the branch on Atlantic Boulevard. Aerial video showed a deputy remove a small object from the bank and place it on a street curb. A bomb-squad member surrounded the device with sand bags, before a robot fired a projectile into the device. Authorities were searching for the two alleged robbers, who reportedly fled in a Kia, possibly white. At least one suspect had a gun. Late the morning of September 5, the area around Atlantic and Whittier boulevards remained closed, and a nearby high school was placed on lockdown. Source: http://www.nbclosangeles.com/news/local/East-LA-Kidnapping-168624296.html

Fake AmEx 'security verification' phishing emails doing rounds. Malicious spam emails impersonating American Express (AmEx) have been hitting inboxes in the last few days, trying to make recipients open an attached HTML file to gather personal information, Help Net Security reported September 4. The email purports to be a notification about a —Membership Security Verification, and warns the users that a —slight error has been detected in their AmEx accounts. To make it right — and not lose access to their accounts in the next 48 hours — the victims are urged to download the attached HTML file and open it in a browser. The phishers are looking for every bit of personal and financial data they can get, including the users' name, address, home and work telephone numbers, Social Security number, mother's maiden name and date of birth, users' date of birth, AmEx credit card number, expiration date, card security code, ATM PIN, email address, and the password for it. All of the information submitted on the fake form will be sent to online criminals and subsequently used to steal the identities of victims as well as use their credit card details to conduct fraudulent transactions, according to Hoax-Slayer. Source: http://www.net-security.org/secworld.php?id=13520

Chemical and Hazardous Materials Sector

Pentagon maps Japan radiation, says U.S. personnel safe. The Pentagon September 5 posted a Web site mapping the amount of radiation to which the tens of thousands of Americans in Japan at the time of 2011's earthquake and Fukushima nuclear disaster were exposed and said none of the doses posed health risks. The Web site showed radiation dosages between March 12 and May 11, 2011 at 13 locations in Japan where most of the nearly 70,000 U.S. military-

affiliated population lived. It showed the highest rate of adult exposure at Camp Sendai, just north of Fukushima, where the estimated adult dose of whole body radiation was 0.12 rem and 1.20 for the thyroid. By comparison, a full-body CAT scan yields a whole body exposure of 5.0 rem. The Pentagon said that by the end of the year it will issue final radiation dose estimates, including estimates for some 8,000 people who had their external or internal radiation measured directly. Source: http://www.reuters.com/article/2012/09/05/us-usa-japan-radiation-idINBRE8841JV20120905

(Louisiana) **Coast Guard investigating 90 reports of oil, chemical leaks following Hurricane Isaac.** The Coast Guard is investigating about 90 reports of oil and chemical releases associated with Hurricane Isaac, including a leak from a closed storage facility in Plaquemines Parish, Louisiana, which killed several brown pelicans, officials said September 4. Separately, the Louisiana Department of Wildlife & Fisheries closed a stretch of coastline from Elmer's Island to Belle Pass after a tar mat appeared in the Gulf of Mexico and tar balls washed ashore. The closure affects commercial and recreational fisheries from the shore to 1 mile offshore. The agency and State Department of Environmental Quality will determine the source of the oil, but its location has stoked concerns that it is remnants of the 2010 Deepwater Horizon explosion and subsequent oil leak. A —defunct terminal with storage tanks at Myrtle Grove leaked oil that has been contained, said the commander of Coast Guard Sector New Orleans and captain of the port of New Orleans. Other reports range from lose barrels to overturned rail cars and tanks that are not leaking. He also cited a chemical release in Braithwaite. Source: http://www.nola.com/hurricane/index.ssf/2012/09/coast_guard_investigating_90_r.html

Commercial Facilities

(Oregon) **Monster truck mishap in Ore. sends 3 to hospital.** A large four-wheel-drive truck veered out of control during a race at Harrisburg MotorSports Complex in Harrisburg, Oregon, struck a barrier, and crossed into the spectator area, where three people were injured, authorities said. The three hurt September 1 were taken to a hospital, said a Linn County sheriff. Sheriff's officials said their injuries were not life-threatening. The 1975 Ford pickup, fitted with large tractor tires, had slowed to about 10 mph just before coming to a stop, the sheriff said. Emergency crews responded to the complex about 30 minutes after —Monster Air 2012 began. The owner of the complex said numerous precautions had been taken to keep spectators safe. However, he said the truck's hydraulic steering went out suddenly during a two-truck race and that the driver could not stop it as it veered into the spectator area. He said about 1,000 people attended the event. Source: http://beatricedailysun.com/news/national/monster-truck-mishap-in-ore-sends-to-hospital/article_aafa3f41-2067-5696-b4e5-e8c8f8d8674c.html

Communications Sector

Phone-focused cyber-criminals move to premium scams. Mobile devices are typically of limited value to online criminals who are driven by money. However, criminals in China, Russia, and Eastern Europe have found a model that appears to be particularly effective: Using

malware to charge for fraudulent premium services. Known as toll fraud, the technique has increased exponentially, accounting for 79 percent of all malware detected by mobile security firm Lookout, the company stated in a report released September 6. Fake installers are the primary method for infecting users and have likely brought in millions of dollars from victims in Eastern Europe and Russia, according to Lookout. In the United States, malicious Web links and aggressive advertising are far more common, Lookout found. Source: http://www.eweek.com/c/a/Security/PhoneFocused-CyberCriminals-Move-to-Premium-Scams-513272/

Hacker group claims access to 12M Apple device IDs. Hacker group AntiSec published what it claims is about 1 million unique device identifier numbers (UDIDs) for Apple devices that it said it accessed earlier in 2012 from a computer belonging to an FBI agent. The group, which is a splinter operation of the Anonymous hacking collective, claims it culled more than 12 million UDIDs and personal data linking the devices to users from the FBI computer. AntiSec said it chose to publish a portion of those records to prove it has them. In a note on Pastebin, a member of AntiSec said the group culled some personal data such as full names and cell numbers from the published data. Instead, the group said it published enough information such as device type, device ID, and Apple Push Notification Service tokens to let users determine whether their devices are on the list. It was not immediately possible to verify the authenticity of AntiSec's claims about the data. Source: http://www.computerworld.com/s/article/9230883/Hacker_group_claims_access_to_12M_Apple_device_IDs

Google suspicious sign-in alert contains a trojan. Unknown attackers are attempting to persuade email recipients to open attachments that contain a trojan by claiming to be from The Google Accounts Team. A new email supposedly from —accounts-noreply@google(dot)com with the subject —Suspicious sign in prevented is being sent en masse, claiming a hijacker attempted to access the mail recipient's Google Account. The message says the sign-in attempt was prevented but asks users to refer to the attached file for details of the attempted intrusion. However, instead of containing information such as the IP address of the log-in attempt, the attached zip file contains a Windows executable file that will install a trojan onto a victim's system. While Google does sometimes send emails like this to users, they never contain attachments; users that receive such an email are advised to delete them. According to VirusTotal, the trojan is currently only detected by just half of 42 anti-virus programs used by the online virus scanner service. Source: http://www.h-online.com/security/news/item/Google-suspicious-sign-in-alert-contains-a-trojan-1698349.html

VMware secures server products. VMware released an advisory, VMSA-2012-0013, which addresses vulnerabilities in open source components in its VMware vCenter 4.1, VMware vCenter Update Manager 4.1, VMware ESX and ESXi, and VMware vCOps 5.0.2 or earlier. Among the upgraded components are OpenSSL, Perl, libxm2, and the Linux kernel. Source: http://www.h-online.com/security/news/item/VMware-secures-server-products-1698343.html

Critical Manufacturing

Ford recalls more Escapes on engine issues. Ford recalled its brand new 2013 Escape for the third time in 2 months, once again citing engine problems that could lead to a fire, FOXBusiness reported September 6. The report includes 7,600 Escape vehicles equipped with 1.6 liter engines. The Detroit automaker said the cylinder head cup plug, also known as the freeze plug, in the engine's cooling system may become dislodged, resulting in —significant loss of engine coolant. As the coolant leaks, it could evaporate on the hot engine, causing the glycol to ignite and leading to an engine compartment fire. In July, Ford recalled 11,600 Escapes for faulty engine compartment fuel lines, and 10,000 for a brake pedal interference issue. Source: http://www.foxbusiness.com/industries/2012/09/06/ford-recalls-another-6000-new-escapes-on-engine-issues/

Two Chinese nationals charged in U.S. Two Chinese nationals face federal charges for allegedly trying to steal trade secrets from Pittsburgh Corning's plant in Sedalia, Missouri. The two, both citizens of China, were charged with attempting to pay $100,000 for the stolen trade secrets from the Sedalia plant, which makes FOAMGLAS, said the acting U.S. attorney, the U.S. Justice Department said on its Web site. The two were charged in a federal criminal complaint, alleging they tried to illegally buy trade secrets for the purpose of opening a plant in China to compete with Pittsburgh Corning. The two were arrested in their hotel room August 26 by the FBI, the report said. The various grades of cellular glass insulation sold under the trade name FOAMGLAS are used to insulate industrial piping systems and liquefied natural gas storage tank bases largely used by energy and petro chemical companies and by natural gas facilities, the report said. The report said Pittsburgh Corning recently reported technological advances in these products and that the company treats its product formula and manufacturing process as proprietary and trade secrets. The report said Pittsburgh Corning is in negotiations to build a plant in China. Source: http://www.upi.com/Top_News/US/2012/09/05/Two-Chinese-nationals-charged-in-US/UPI-26711346817976/

(Pennsylvania) **Hacker hands Barto manufacturer $190,000 loss.** A hacker broke into a Berks County, Pennsylvania manufacturer's computer system and stole nearly $200,000, according to State police. The Reading Eagle reported September 3 that the banking system at CWI Railroad System Specialists, a company that manufactures train engine parts, was hacked in August, troopers said. The hacker entered the system and issued payments to banks in Virginia. Investigators were able to track the origin of the attack using the attacker's Internet protocol address. A total of $190,000 was sent to four banks August 24 and 27, investigators said. —Malware must have been placed somewhere to make the withdrawal, CWI's vice president said. —There is only one computer in our company that has access to our Quaker National Bank account. I don't know how they could have gotten to it. According to investigators, people were waiting at the banks to either deposit the money into an account or cash the checks. Source: http://readingeagle.com/article.aspx?id=412706

Defense/ Industry Base Sector

Nothing Significant to Report

Emergency Services

(Michigan) **Prison still under quarantine as illnesses spread.** Nearly 100 people, counting prisoners and staff at the Saginaw Correctional Facility in Freeland, Michigan, were battling E-coli infections. The outbreak was first noticed the week of August 27, and shortly after that the facility was quarantined to prevent the spread. Eighty-nine prisoners and seven staff members were suffering from nausea and diarrhea. Local and State health departments were investigating and said this strand of E-coli is particularly nasty, and there is no treatment. Four people have been hospitalized. The illness is usually spread through food. A representative for the Corrections Department said all food is prepared on-site in the prison kitchen. No new cases have been reported recently, but the incubation period for the illness is 3 to 7 days. Once a week passes without a new diagnosis, the quarantine will be lifted and normal activity and visiting hours at the prison will resume. Source: http://www.wnem.com/story/19456646/prison-under-quarantine-as-illnesses-spread?hpt=us_bn9

(Alabama) **Alabama first state to scan fingerprints of prison visitors.** The Alabama Department of Corrections has enacted a first-in-the-nation policy requiring visitors at the State's prisons to have their fingerprint scanned before they are allowed to enter the facilities, USA Today reported September 5. No other State prison system has a similar requirement. The change, implemented in August, has its roots in the prison system getting a new computer program, said a spokesman for the Department of Corrections. He stated, —We still require visitors to have a government-issued photo ID, and that requirement will remain in place. But there are times when someone else resembles the photo on an ID. Scanning the fingerprint of visitors verifies they are who they say they are. Alabama prison visitors' fingerprints will not be filed in a database, and the prints will not be shared with other local, State, or national law enforcement agencies, the corrections spokesman said. Source: http://www.greenvilleonline.com/usatoday/article/57587480?odyssey=mod|newswell|text|News|p

Energy

Insiders suspected in Saudi cyber attack. One or more insiders with high-level access are suspected of assisting hackers who damaged some 30,000 computers at Saudi Arabia's national oil company in August, sources familiar with the company's investigation say, Reuters reported September 7. The attack using a computer virus known as Shamoon against Saudi Aramco — the world's biggest oil company — is one of the most destructive cyber strikes conducted against a single business. Shamoon spread through the company's network and wiped computers' hard drives clean. Saudi Aramco says damage was limited to office computers and did not affect systems software that might hurt technical operations. The hackers' apparent

access to a mole, willing to take personal risk to help, is an extraordinary development in a country where open dissent is banned. Hackers from a group called —The Cutting Sword of Justice claimed responsibility for the attack. They say the virus gave them access to documents from Aramco's computers, and have threatened to release secrets. Reports of similar attacks on other oil and gas firms in the Middle East, including in neighboring Qatar, suggest there may be similar activity elsewhere in the region, although the attacks have not been linked. Source: http://in.reuters.com/article/2012/09/07/net-us-saudi-aramco-hack-idINBRE8860CR20120907

Oil and gas production ramping up after Isaac. The nation's oil and gas hub along the Gulf Coast is slowly coming back to life in the aftermath of Hurricane Isaac, the Associated Press reported September 3. Offshore oil platforms are beginning to ramp up production as crews are returning. Refineries are beginning to restart units as power is restored and floodwaters are cleared out. The Bureau of Safety and Environmental Enforcement said September 3 that 800,000 barrels per day of oil production remained offline, 58 percent of Gulf of Mexico production. About 100,000 barrels per day of production was restored between September 2-3. At the height of the storm, 1.3 million barrels per day of oil production was suspended. About 12 percent of the region's platforms were still without staff. Onshore pipelines, ports, and terminals have re-opened, though some are still operating with restrictions, the Energy Department said. Several natural gas pipelines remained shut, along with natural gas processing plants that depend on gas from the pipelines. The Energy Department reported that most operators anticipate gas flows resuming over the next few days. Source: http://www.businessweek.com/ap/2012-09-03/oil-and-gas-production-ramping-up-after-isaac

Food and Agriculture

Soybean sprouts and tofu recalled for Listeria. Newark, New Jersey-based Manna Organics, Inc. September 2 recalled various soybean sprouts and tofu products because they have the potential to be contaminated with potentially deadly Listeria monocytogenes. Manna Organics became concerned about possible contamination after random testing by the New York State Department of Agriculture and Markets discovered Listeria in a package of of Soonyeowon Soybean Sprouts. The company suspended production while it investigated the problem with the U.S. Food and Drug Administration. The recalled products were distributed to various restaurants, retailers, and distributors in New York, New Jersey, Pennsylvania, Massachusetts, Virginia, Maryland, Connecticut, Georgia, Illinois, and Texas on or after July 17. Source: http://www.foodsafetynews.com/2012/09/soybean-sprouts-and-tofu-recalled-for-listeria/#.UEX10aC6TlY

Government Sector (including Schools and Universities)

(New Jersey) **White powder causes concern at county courthouse.** A hazardous materials crew responded September 6 to the Burlington County, New Jersey Courthouse in Mount Holly after a man tried to enter the building with a bag full of white powder. He immediately was stopped

by county sheriff's officers and never entered the building, officials said. The powder was tested and turned out to be cornstarch, a county spokeswoman said. The man told the officers he was taking the bag to the Burlington County Prosecutor's Office in the seven-story building, but then changed his story, officials said. Authorities wanted the man evaluated for mental health concerns. Source: http://www.phillyburbs.com/news/local/burlington_county_times_news/breaking_news/white-powder-causes-concern-at-county-courthouse/article_2ed4384b-475d-5912-b8e4-34abf1e1945c.html

Pentagon: Bin Laden book has classified info. A former Navy SEAL's insider account of the U.S. raid that killed a notorious terrorist contains classified information, the Pentagon press secretary told reporters September 4. The Pentagon spokesman said that an official review of the book determined that it reveals what he called —sensitive and classified information. He said the book should have been submitted to the Pentagon before publication for a formal review of potential disclosures. A lawyer for the author has disputed that he was legally obliged to have the book screened before publication. Source: http://thechronicleherald.ca/world/132825-world-in-brief-september-5-2012

US FBI to lead Pakistan blast probe. The FBI will lead the probe into a suicide car bomb attack on an American diplomatic car in Pakistan that killed two people, U.S. officials said September 5. The FBI team will work alongside Pakistani investigators as they search for clues to who was behind the September 3 blast in the northwestern city of Peshawar, in which an attacker rammed his explosives-laden car into a U.S. consulate vehicle. Two American and two Pakistani consulate employees were wounded in the bombing. No group has yet claimed responsibility, but militants linked to the Taliban and Al Qa'ida have targeted the consulate and its staff at least twice before since April 2010. Source: http://www.google.com/hostednews/afp/article/ALeqM5j0JTWq6huZ_PjitzMGT_wqUxY-RQ?docId=CNG.5d2ec792377aa5e4409a15b3d69dd102.4a1

Information Technology and Telecommunications

(North Carolina) **North Carolina man accused of Twitter threats to kill President.** A North Carolina man was arrested September 5 and accused of threatening to kill the U.S. President in a series of Twitter messages. He had an initial court appearance in Charlotte September 6 and remains in custody. According to a criminal complaint, he sent five Twitter messages September 3 threatening the President, 2 days before the President arrived in Charlotte for the Democratic National Convention. The court document states a Secret Service intelligence research specialist saw the messages on Twitter, which led to an agent going to the suspect's home to interview him September 5. —[The suspect] stated that he published the statements because he hated [the President], a Secret Service agent wrote in the affidavit. —[He] asserted that he was high on marijuana when he made the threats but that he understood what he was doing and that it was wrong. According to the court document, the agent then arrested him on several outstanding warrants. The officer said the suspect's demeanor changed and the suspect

asserted he was sorry he sent the messages. Source: http://www.cnn.com/2012/09/06/justice/obama-threat-arrest/index.html

BYOD security monitoring is not the norm. More than 82 percent of federal computer security professionals have policies for safeguarding government data on employees' personal smartphones — but most have no idea whether those policies are being followed every day, according to a new study released September 6 by cybersecurity compliance firm nCircle. About 90 percent of participants who had bring-your-own-device, or BYOD, security policies said they were enforcing them. Enforcement for personal devices probably involves simply spot checking security posture and other periodic oversight, said nCircle's director of federal markets. Only 62 percent of respondents said they have a strategy for conducting continuous monitoring. —Part of the issue is our standards have gone up, she said. Continuous monitoring became a requirement less than 3 years ago. —If you look at the mobile device arena, it's very complex. You have five or six different operating systems that you need to monitor, she added. Each brand has widely different approaches to encrypting data and verifying user identities. To gather insights, nCircle surveyed online and interviewed more than 100 government security workers, including risk and audit managers, senior executives, and contractors. The study was conducted between April and July. Source: http://www.nextgov.com/cybersecurity/2012/09/byod-security-monitoring-not-norm/57923/?oref=ng-channelriver

Norton: Cybercrime cost $110 billion last year. The yearly Norton Cybercrime report analyzes how cybercrime affects consumers, and how emerging technology — including mobile and cloud computing — impacts security. As mobile technology and bring your own device (BYOD) schemes insinuate themselves into the corporate sphere — blending personal and professional communication — businesses must take note. The 2012 report consists of more than 13,000 participants across 24 countries, aged 18-64, and says that U.S. consumers lost $20.7 billion in 2011 after falling prey to cybercrime including attacks, malware, and phishing. Globally, the rate rose to $110 billion in direct financial loss. An estimated 71 million people in the United States became cyber crime victims in 2011. Source: http://www.zdnet.com/norton-cybercrime-cost-110-billion-last-year-7000003745/

New attack uses SSL/TLS information leak to hijack HTTPS sessions. There is a feature supported by the SSL/TLS encryption standard and used by most of the major browsers that leaks enough information about encrypted sessions to enable attackers decrypt users' supposedly protected cookies and hijack their sessions. The researchers who developed the attack that exploits this weakness said all versions of TLS are affected, including TLS 1.2, and the cipher suite used in the encrypted session makes no difference in the success of the attack. The attack was developed by the same pair of researchers who in 2011 released details of a similar attack on SSL/TLS and wrote a tool called BEAST, which also gave them the ability to decrypt users' cookies and hijack sessions with sensitive sites such as e-commerce or online banking sites. Source: http://threatpost.com/en_us/blogs/new-attack-uses-ssltls-information-leak-hijack-https-sessions-090512

Apple Java update fails to address mega-flaw – researcher. Apple released an update for Java September 5, but it does not tackle a high-profile flaw that has become the target of attacks over recent weeks. Java for OS X 2012-005 and Java for Mac OS X 10.6 Update 10 offer patched versions of Java for OS X Lion and Mountain Lion systems that tackle CVE-2012-0547. However, this is a different problem than the CVE-2012-4681 bug currently targeting Java users, Krebs on Security reports. Source: http://www.theregister.co.uk/2012/09/06/apple_java_update/

Secret account in mission-critical router opens power plants to tampering. DHS' Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) warned power utilities, railroad operators, and other large industrial players of a weakness in a widely used router that leaves them open to tampering by untrusted employees. The line of mission-critical routers manufactured by Fremont, California-based GarrettCom contains an undocumented account with a default password that gives unprivileged users access to advanced options and features, an expert in the security of industrial control systems told Ars Technica. The —factory account makes it possible for untrusted employees or contractors to significantly escalate their privileges and then tamper with electrical switches or other industrial controls that are connected to the devices. ICS-CERT issued an advisory recommending that users of the GarrettCom devices install a security update that locks down the factory account. Source: http://arstechnica.com/security/2012/09/secret-account-in-mission-critical-router-opens-power-plants-to-tampering/

FBI denies report hackers leak 1 million Apple device IDs. September 4, the FBI disputed a computer hacker group's claim that it stole personal identification data on millions of Apple device owners from an FBI agent's laptop. FBI officials said the bureau never asked for and never possessed the database that the group, which calls itself AntiSec, posted on a Web site. —The FBI is aware of published reports alleging that an FBI laptop was compromised and private data regarding Apple UDIDs was exposed, a spokeswoman told Fox News. —At this time, there is no evidence indicating that an FBI laptop was compromised or that the FBI either sought or obtained this data. The group released a link to a database of more than 1 million unique identification numbers for Apple devices, which could include iPhones and iPads. AntiSec said the data is just a piece of the more than 12 million unique identification numbers and personal information on the device owners that the group obtained from a laptop used by an FBI agent. The FBI denied it ever had that information. Officials with the bureau said they could not verify the validity of the data AntiSec released. Federal officials also warned that computer users should be careful when clicking on such links because they sometimes may contain malware that can infect computers. Source: http://www.foxnews.com/tech/2012/09/04/hackers-leak-1-million-apple-device-ids/?intcmp=obnetwork

Philips databases pillaged and leaked second time in a month. Electronics giant Philips was hacked for the second time in a month and its databases raided. Usernames and encrypted passwords were leaked after the breach. It is unclear whether email addresses or the actual contents of corporate emails were included in the records dumped from the company's SQL databases. The lifted data was uploaded to various file hosting sites by hacktivists, who used

blogs (since taken down by Google's Blogspot service) and social networks, using the hashtag labels —AntiSec and —LulzSecReborn to spread the word. —All together there is [sic] well over 200,000 emails with at least 1,000 of them have further vital credentials that could allow others to use the users' personal information, according to a Web site run by Anonymous. The site reports that Anonymous-affiliated hackers in Sweden announced the raid. The latest attack follows a smaller leak of a few thousand records from Philips by r00tbeersec, another hacktivist crew, about a week ago. Source: http://www.theregister.co.uk/2012/08/31/philips_anon_hack/

National Monuments and Icons

(California) **3rd Yosemite visitor dies of hantavirus.** Officials announced two new cases of hantavirus infection linked to Yosemite National Park in California after health authorities confirmed them September 6, a park spokesman said. One case resulted in a fatality, which was reported by the Kanawha-Charleston Health Department in West Virginia, the Los Angeles Times reported September 7. A park spokesman said the victim stayed in one of 91 —signature tent cabins in Curry Village in mid-June. Park officials have attributed seven of the eight cases of hantavirus pulmonary syndrome — three of which have been fatal — to the insulated signature tent cabins and warned that anyone who stayed there between June 10 and August 24 was at risk. The other newly reported infection was linked to camps along the High Sierra Loop, a route frequented by backpackers. Now Yosemite officials are sending emails and letters to about 6,000 people who stayed in the High Sierra Camps and the Tuolumne Meadows Lodge this summer, the spokesman said. The 91 signature tent cabins in Curry Village were cleared the week of August 27 as crews cleaned and retrofitted them to fill gaps that allowed mice inside the insulated walls. They remain closed indefinitely. Source: http://www.morrisdailyherald.com/2012/09/07/3rd-yosemite-visitor-dies-of-hantavirus/a9llfmv/

(California) **CDC says 10,000 at risk of hantavirus in Yosemite outbreak.** Some 10,000 people who stayed in tent cabins at Yosemite National Park in California this summer may be at risk for the deadly rodent-borne hantavirus, the U.S. Centers for Disease Control and Prevention (CDC) said August 31. The CDC urged lab testing of patients who exhibit symptoms consistent with the lung disease, hantavirus pulmonary syndrome, after a stay at the park between June and August and recommended that doctors notify state health departments when it is found. Two men have died from hantavirus linked to the Yosemite outbreak and four others were sickened but survived, while the CDC said additional suspected cases were being investigated from —multiple health jurisdictions. Most of the victims were believed to have been infected while staying in one of 91 —Signature tent-style cabins in Yosemite's Curry Village camping area. —An estimated 10,000 persons stayed in the _Signature Tent Cabins' from June 10 through August 24, 2012, the CDC said. Nearly 4 million people visit Yosemite, one of the nation's most popular national parks, and roughly 70 percent of those visitors congregate in Yosemite Valley, where Curry Village is located. Source: http://www.reuters.com/article/2012/08/31/us-usa-hantavirus-yosemite-idUSBRE87U04P20120831

(Idaho; Montana) **3 big Idaho wildfires resist containment efforts.** Firefighters in Idaho continue to battle three large wildfires that were proving difficult to bring under control, the Associated Press reported September 2. In central Idaho, the 194-square-mile Halstead Fire was only 7 percent contained and September 2 was about 100 yards from power lines that provide power to the mountain tourist town of Stanley. The Custer County Sheriff's Office September 1 told residents of about 30 homes between Sunbeam and Yankee Fork to evacuate. To the south, back burns on the 226-square-mile Trinity Ridge Fire have been effective in protecting Featherville and an evacuation order was lifted September 2. Crews were trying to slow the fire's growth toward the Middle Fork Boise River. About 1,200 personnel were assigned to the fire that was 31 percent contained. Along the Idaho-Montana border, fire managers said the 329-square-mile Mustang Complex of fires would be difficult to contain without rain or snow. Fire officials August 29 issued various evacuation levels for residents near the fire that remained in effect. Residents along Highway 93 between Hull and Sheep were advised to leave immediately. More than 900 wildland firefighters were fighting the blaze that was 16 percent contained and has burned across the Idaho border into Montana. Source: http://www.statesmanjournal.com/viewart/20120902/UPDATE/120902014/3-big-Idaho-wildfires-resist-containment-efforts?odyssey=tab|topnews|text|News

Postal and Shipping

Nothing Significant to Report

Public Health

(Texas) **Hospital district patient names sold in Medicare scheme.** The Houston Chronicle reported August 31 that the Harris County Hospital District August 30 notified approximately 3,000 patients that their information, including addresses, phone numbers, dates of birth, and Social Security numbers, may have been stolen by a former employee indicted in federal court in a Medicare kickback scheme involving 2 home health care operators. —The alleged misuse of the information, as far as the hospital district knows at this time, was designed by the former employee to defraud Medicare and not patients, according to a statement issued by the hospital district. The former employee was among 107 people named in a nationwide Medicare fraud sweep in May. He was accused of selling patient information to the owner of Jackson Home Healthcare who would, in turn, disclose that information to others, including the employees of Houston Compassionate Care Inc. Source: http://www.chron.com/news/houston-texas/article/Hospital-district-patient-names-sold-in-Medicare-3829012.php

Transportation

(Ohio) **Three anarchists plead guilty to Ohio bridge bomb plot.** Three self-described anarchists pleaded guilty September 5 in an Ohio federal court to plotting to blow up a four-lane highway bridge near Cleveland in April, authorities said. The suspects pleaded guilty to conspiracy to use a weapon of mass destruction, attempted use of a weapon of mass destruction, and attempted use of an explosive device to destroy property used in interstate commerce, authorities said in

a statement. The three guilty pleas came before a U.S. district judge who expects to sentence the men in November. All three had been scheduled to face trial September 17. Five men in all were accused of plotting to blow up a bridge 30 miles south of Cleveland that runs through Cuyahoga Valley National Park. A fourth suspect pleaded guilty in July to the attempted attack and agreed to testify against the others. The fifth suspect is undergoing competency testing. Source: http://whtc.com/news/articles/2012/sep/05/three-suspects-plead-guilty-to-ohio-bridge-bombing-plot/

(Massachusetts) **Homeland Security testing new bioagent sensors in Boston subway line.** The DHS has begun vetting several new bioagent detection systems that could one day be deployed at airports, subway stations, and other locations around the United States, Global Security Newswire reported September 6. Roughly 60 sensors have been dispersed in Boston subway stops. A first round of testing was conducted the week of August 27, and trials are expected to continue on a regular basis for 6-8 months, said a spokesman for the DHS Science and Technology Directorate. The tests are intended to determine whether sensors produced by four different companies could detect the terrorist release of a lethal biological agent. Homeland Security specialists, in this case, are releasing an inert, harmless bacteria after the subway line shuts down each day. Three of the devices being tried out check the air on a nonstop basis for changes to atmospheric content that would indicate a dangerous biological agent is present. The fourth type analyzes air samples to confirm the existence of such a threat, he said. The technologies could ultimately be acquired and installed by public health agencies, transit operations, and other organizations. Homeland Security's findings from the test program will be provided to those potential users. The sensors would be fielded indoors as a complement to devices already in place in about 30 cities under the department's Biowatch program. Source: http://www.nti.org/gsn/article/homeland-security-testing-new-bioagent-sensors-boston-subway-line/

(Pennsylvania) **Police: 2 arrested in Butler County railroad wire theft.** Two people were accused of stealing copper wire from railroad tracks near McCandless Road in Slippery Rock Township, Pennsylvania, WPXI 11 Pittsburgh reported August 31. One individual was accused of removing 900 feet of copper wire from the Canadian National Railroad and selling it, according to police reports. Officers said the other individual assisted in the sale of the stolen copper and was being charged with receiving stolen property and conspiracy. Canadian National has fixed the railroad, replacing the wire, according to officials. Source: http://www.wpxi.com/news/news/2-arrested-butler-county-railroad-wire-theft/nRQjS/

Bird-airplane collisions are up five-fold since 1990. There are more planes and more large birds flying, and collisions between them are happening five times more often than they did in 1990, sometimes with deadly results, a new federal report said. Almost 75 commercial planes have hit birds in 2012 while taking off or landing at Washington D.C.'s three major airports alone, and in more than a dozen instances in the past 5 years, aircraft have suffered major damage, the Washington Post reported September 4. The Federal Aviation Administration (FAA) has spent $458 million in the past 5 years to control birds and other wildlife around airports, but an inspector general's report said it must do a better job. The FAA said it plans to tighten its

oversight. The U.S. Department of Agriculture, working on behalf of the FAA, has taken measures to reduce airport wildlife. Keeping the critters at bay is no easy task. Failure to do so carries a cost: an estimated $625 million a year and at least 25 deaths and 235 injuries since 1988. Source: http://www.adn.com/2012/09/03/2610044/bird-airplane-collisions-up-five.html

DOT orders shutdown of reincarnated Tennessee carrier. The Federal Motor Carrier Safety Administration (FMCSA) ordered Tennessee-based trucking company Terri's Farm to immediately cease all interstate transportation services, based on evidence it was a chameleon operation for an unsafe company previously shut down by the agency, Trucking Info reported September 4. Following a thorough review, FMCSA shut down Terri's Farm after finding it was operating the same vehicles and maintaining the same operational and safety management structure as former horse transporter Three Angels Farms. June 29 FMCSA ordered Three Angels Farms, its officers, and vehicles out of service after safety investigators found multiple safety infractions, including allowing drivers to operate commercial motor vehicles without commercial driver's licenses, and not conducting controlled substances testing of drivers. In the past 8 months, the former Three Angels Farms had two accidents involving poorly maintained vehicles and fatigued or disqualified drivers that resulted in the deaths of four horses. —Terri's Farm's operational structure and safety management controls are a continuation of the inadequate safety management controls of Three Angels Farms, read the order. The notice said that failure to comply could result in civil penalties of up to $16,000 per day for each day the companies continue operating in violation of the order. Source: http://www.truckinginfo.com/news/news-detail.asp?news_id=77897

Water and Dams

Nothing Significant to Report

Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168